EDUCAUSE

Docket No. 100402174
Notice of Inquiry

June 7, 2010

Attention: Internet Policy Task Force
National Telecommunications and Information Administration
U.S. Department of Commerce

Dear Members of the Internet Policy Task Force:

Thank you for the opportunity to submit comments in response to the Department's review on Information Privacy and Innovation in the Internet Economy. We respectfully submit these comments on behalf of EDUCAUSE – a non-profit organization whose mission is to advance higher education by promoting the intelligent use of information technology.

We are writing to express the views of the higher education information technology and privacy community regarding the strategic and operational impact of information privacy and the Internet economy upon our nation's colleges and universities. We recognize that the Department has consulted many academic experts – faculty who come from our community of institutions whose academic discipline, research, and experience lend incredible expertise; however, we represent the voice of campus administrators and higher education leaders who can speak on the importance of innovation, privacy practices, and the Internet economy to the future of higher education.

Higher education, working with the federal government, established high speed data networks for research and education. The deployment of information technologies has transformed higher education through learning technologies that support curriculum and distance education, online libraries and digital repositories, and software applications for administration and research or grid computing. The increased leverage of commercial applications for enterprise systems and ongoing experiments with a variety of platforms for cloud computing requires standards for privacy and security that reflect higher education's interest in protecting its constituents and preserving the foundation of our teaching, research, and service missions to American society.

Privacy protections directly impact the higher education community, its students, employees, and guests. Current privacy law and regulation is overly complex and confusing, where higher education institutions are governed by numerous and varied laws, institutional policies, and local institutional cultures. We strongly feel that there is a need for standardization and clarity to today's privacy framework in order to preserve and facilitate further innovation in the higher education sector.

1150 18th St. NW, Suite 1010
Washington, DC 20036
Main 202.872.4200
Fax 202.872.4318

4772 Walnut St., Suite 206
Boulder, CO 80301
Main 303.449.4430
Fax 303.440.0461

educause.edu

We would like to briefly address some of the issues raised in the Request for Comment.

1. The U.S. Privacy Framework Going Forward

The application of privacy practices in colleges and universities draws upon a combination of approaches: voluntary adoption and promotion of fair information privacy practices; compliance with a diverse array of state, federal, and foreign laws and regulations; and other legal or contractual requirements. Additionally, core academic values in our institutions (e.g., academic and intellectual freedom, ethics, research on human subjects, social responsibility, etc.) typically adhere to heightened standards of privacy protections that extend beyond minimal legal requirements. However, the "consumers" of the programs and services offered at a college or university bring privacy expectations that are shaped by their experiences in commerce, government, and other sectors of the economy. Thus, colleges and universities are increasingly impacted by a fragmented compliance regime that regulates our sector according to the type of information we collect and maintain (e.g., health, financial, education records, etc.).

There is also concern among administrators that these obligations are imposing "unfunded mandates" during a time where demands on funding exceed resources available. We support a comprehensive privacy framework that transcends sectors of the economy that will simplify compliance, minimize costs for not-for-profit institutions, and maximize appropriate privacy protections for individuals.

2. U.S. State Privacy Laws

Public or state-assisted higher education institutions may be subject to state laws and local requirements depending upon their independence or status as a state agency. All institutions may be subject to data privacy or security laws depending on the scope of the legislation. The application of state privacy and information security laws to colleges and universities is complicated by the fact that while the locus of operations for an institution is typically limited to a single state, the students who attend these institutions come from states across the nation. Therefore, security breach notification laws (enacted in at least 46 different states) create a confusing and complicated legal and regulatory landscape. The advent of the Internet for use in interstate commerce, including educational applications such as distance education and collaborative research programs, will require more uniform, federal approaches to mitigate the challenges of implementing a fragmented set of diverse state laws.

3. International Privacy Laws and Regulations

As colleges and universities expand their academic, research, and service missions overseas, we are particularly mindful of the complexity of foreign and multinational privacy regimes. Some colleges and universities are establishing formal campuses abroad, bringing into play privacy compliance in the countries where those campuses are located. More commonly, faculty and students travel to other countries for study or

research for very short durations, often moving from country to country during the course of their visit. Addressing privacy compliance in coordinated international research efforts and academic ventures carried out this way can be especially difficult. Harmonization of data privacy principles and laws would have significant benefit to the higher education community and facilitate global collaboration and innovation for the benefit of society around the world.

4. Jurisdictional Conflicts and Competing Legal Obligations

The complexity of data breach legislation throughout the various states and questions regarding enforcement across state lines is symptomatic of the challenges faced by colleges and universities. Additionally, the lure of "cloud computing" to improve services and reduce costs in higher education is tempered by uncertainties regarding legal jurisdiction that even the providers of cloud computing services are not able to resolve. A significant barrier to the adoption of these innovative and cost effective services by higher education as a whole has been the providers' inability to limit data storage or flow within the boundaries of the U.S.; thus, making the use of these services too risky for higher education.

5. Sectoral Privacy Laws and Federal Guidelines

In addition to the federal laws cited in the Notice of Inquiry (e.g., HIPAA, FCRA, GLBA, COPPA, etc.) that have nuanced applications to institutions of higher education, the Family Education Rights and Privacy Act (FERPA) addresses the privacy of student education records. The Department of Education's Family Policy Compliance Office is responsible for issuing regulations and enforcement. From an institutional perspective, the diverse array of federal regulatory and enforcement agencies (i.e., Department of Health and Human Services, Federal Trade Commission, Department of Education, etc.), combined with the unique approach taken by each data privacy law adds additional levels of complexity that make creating a uniform approach to compliance difficult at the enterprise level.

Although a consumer may be oblivious to how their various types of information are governed by federal law and regulation, they are typically subject to a variety of institutional policies or practices as well, each uniquely designed to protect their privacy in accordance with the compliance obligations imposed on educational institutions. For example, a website privacy policy may exist at the institution's choice or because it is required by state law; a notice of privacy practices may be issued to students who visit the student health center; a policy on student education records may be referenced in course syllabi; a consent form may be required before a student participates in a research project where they are deemed a human subject. While these individual approaches may heighten sensitivity and awareness of the need for privacy protections, they also confuse if not obscure expectations of the consumer for whom they are designed to protect.

6. New Privacy-Enhancing Technologies and Information Management Processes

Colleges and universities have been leaders in the development and use of privacy-enhancing identity management technologies and practices. The National Science Foundation funded the National Middleware Initiative, led by EDUCAUSE and Internet2, in an effort to advance the use of middleware technologies in higher education for purposes of identification, authentication, and authorization. Institutional efforts to centralize data collection and use for identity and access management help to eliminate the unnecessary redundancy of multiple user IDs and passwords for access to individual systems and in the process improve privacy protections for the individual. Increasingly, the move towards more federated systems of identity management, including the use of the InCommon Federation (www.InCommon.org) for research and education networks, creates a trust framework that minimizes the information exchanged between identity providers and relying parties. The community of trust inherent among higher education institutions makes us a good testing ground for the application of inter-institutional federations.

7. Small and Medium-Sized Entities and Startup Companies

While the most well known higher education institutions tend to be large organizations as measured by number of students, employees, scope of activity, and resources, the vast majority of institutions are small to mid-size that include two-year (community) colleges and four-year colleges and universities. These institutions are often resource-constrained and rarely have a chief privacy officer or another individual expert on privacy matters. Fortunately, the size and scope of their operations limit the impact of certain laws that might only apply to larger, research universities. However, they share many of the same challenges with respect to compliance with state, federal, and foreign laws, having to do so with fewer resources.

8. The Role for Government/Commerce Department

We believe that the U.S. Department of Commerce is well-positioned to assess the impediments to commerce and innovation that our current privacy regulatory regime imposes. Where commerce and innovation are overly impeded without compelling privacy gain, the Department should aim to develop solutions. One critical solution that the Department could help lead is to bring together regulatory bodies and other experts domestically and internationally with the goal of harmonizing requirements and facilitating important services, research, innovation that are dependent on the flow of data. In such an effort, we offer the following recommendations for how the work should proceed:

1. Establish principles – not overly prescriptive rules – that protect privacy and advance innovation. Examples include meaningful consent, reasonable access, and security controls that are effective for varying types and sizes of organizations.

2. Differentiate among choice requirements depending upon the type of information and forms of use. In other words, there should be fewer privacy concerns and less need for robust opt-in procedures when an organization is not using data for advertising or marketing purposes or making decisions that significantly impact the individual (such as employment-related uses.) The converse is true as well.

3. Encourage legislation to standardize breach notification standards and procedures.

4. Establish a focus on research activities and how privacy laws should be applied in a way that allows important research to proceed while adequately protecting privacy.

5. Facilitate innovation by developing and supporting methods whereby entities can participate in new, Internet-based systems of collaboration, including the utilization of cloud computing providers who should be incented to abide by regulations and best practices in privacy protection.

6. Promote the simplification and standardization of privacy statements that are understandable to users.

In conclusion, we thank the Internet Policy Task Force for examining these critical issues, especially the impact of the Internet economy on privacy and innovation, both deeply important to our nation's colleges and universities. We look forward to continued work with the Department and the Internet Policy Task Force to formulate policies that will address the privacy challenges we face in higher education.

Sincerely,

Greg Jackson
Vice President, Policy and Analysis